#ROCKYOURMAIL

Introduction

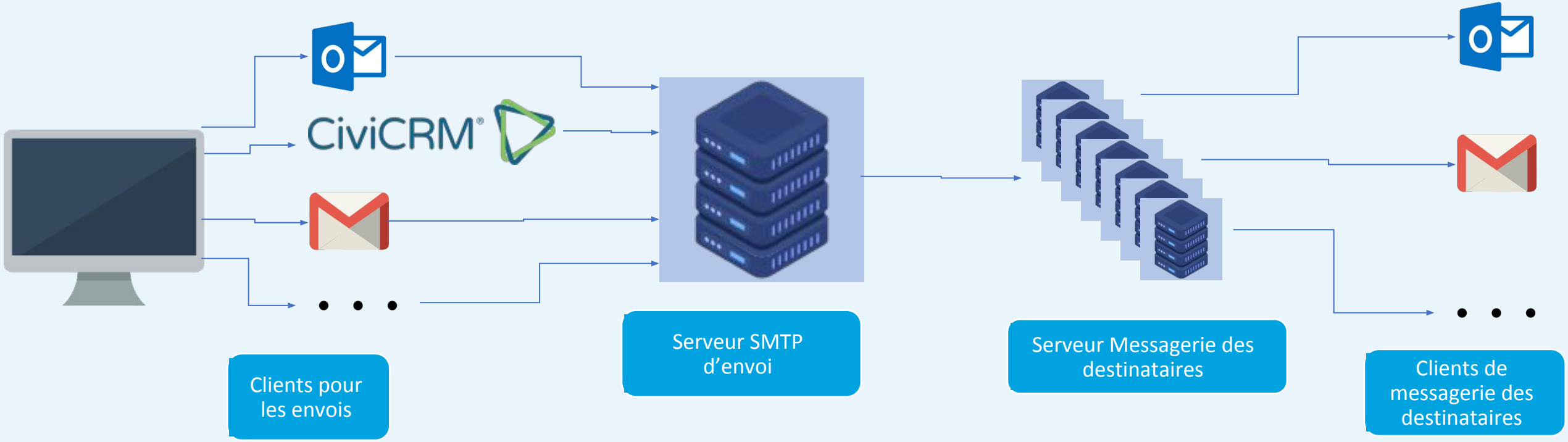
Les bonnes pratiques de l’ emailing

Nous sommes souvent confrontés, lors de l’envoi de campagnes de mails, à de **nombreux rejets de la part des plateformes de nos destinataires.**

Il existe des **moyens d’assurer une meilleure délivrabilité** de nos mails par la **mise en place de règles DNS** et par une **bonne validation du contenu envoyé.**

L’envoi d’une campagne

Comment ça marche ?



Les bonnes pratiques

- Adresse existante pour les envois
- Valider le contenu du mail
- URL dans les mails
- Contenu du mail (texte, images…)

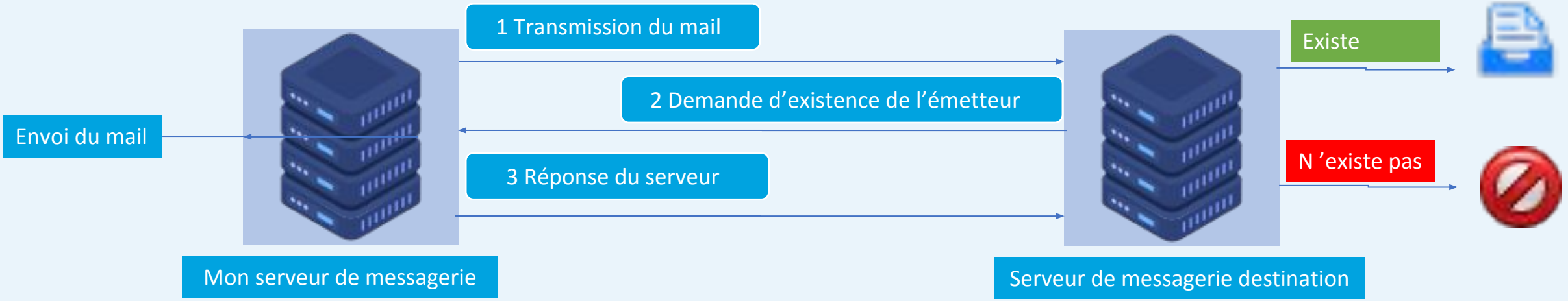
Adresse existante pour les envois

De nombreuses plateformes de messagerie utilise un système de contrôle de l'existence de l'adresse email émettrice appelé « Sender Verify ».
S'il est détecté que l'adresse email n'existe pas, le mail est alors rejeté !

L'avantage d'effectuer ses envois avec une adresse email existante permet de :

1. Recevoir les erreurs suite à des envois vers des adresses erronées/inexistantes
   - Permet de « nettoyer » son CRM d'adresses inutiles
   - Permet de corriger les adresses emails mal orthographiées
2. Pouvoir recueillir les réponses éventuelles des destinataires

Comment ça marche le « sender verify » ?



Valider le contenu du mail

Le travail d'un Anti-Spam

Il y a 2 points de vigilance :

1. **URL de l'email**
    1. **Validité**
    2. **Serveurs reconnus**
2. **Contenu**
    1. **Texte**
    2. **Ratio texte/image**

Au-delà des filtrages euristiques et bayésiens qu'effectuent les anti-spam, ceux-ci vérifient certains éléments du contenu du mails. Ceux-ci peuvent faire augmenter la note de spam d'un mail, voyant donc le risque que celui-ci soit classé en indésirables.

Comment l'éviter ?

URL contenues dans le mail :

1. **Vérifier chaque url avant l'envoi de la campagne, que celles-ci atterrissent bien sur une page existante**
2. **Favoriser des serveurs d'hébergements dont la légitimité est reconnue. Dans l'idéal, il est préférable d'héberger les URL sur le même serveur que son site Web**

Contenu du mail :

3. **Certains mots utilisés ou syntaxes font augmenter les notes de spam :**
   a. **Pharmacie, viagra, médicaments…**
   b. **L'abus de mots en majuscules ou des points d'exclamations !!!!!!**
4. **Il est important que le ratio texte/image favorise toujours le poids du texte**
   a. **Un email comportant juste une image a de forte chance de passer en indésirable**
   b. **Des images de tailles importantes pour peu de texte favorisent un passage en indésirable**

Introduction des réglages techniques

Le fait d'utiliser son propre serveur SMTP ou le serveur SMTP d'un tiers reconnu ne suffit pas à garantir la bonne distribution de ses campagnes.

Il est nécessaire, voire impératif, d'effectuer des réglages au niveau DNS, afin de déclarer des entrées associant le domaine de messagerie aux serveurs SMTP utilisés.

Les plus répandus sont :

1. SPF
2. SKIM

Le SPF

Sender Policy Framework (SPF) est une norme de vérification du nom de domaine de l'expéditeur d'un courrier électronique, normalisée dans la RFC 72081 L'adoption de cette norme est de nature à réduire le spam.

La mise en place doit se faire en collaboration avec les différents prestataires utilisés pour le courrier sortant :

1. Fournisseur de messagerie
2. Fournisseur de passerelle SMTP d’emailing.

Le protocole Simple Mail Transfer Protocol (SMTP) utilisé pour le transfert du courrier électronique sur Internet ne prévoit pas de mécanisme de vérification de l'expéditeur, c'est-à-dire qu'il est facile d'envoyer un courrier avec une adresse d'expéditeur factice, voire usurpée. SPF vise à réduire les possibilités d'usurpation en publiant, dans le DNS, un enregistrement (de type TXT)[3] indiquant quelles adresses IP sont autorisées ou interdites à envoyer du courrier pour le domaine considéré.

Source Wikipédia

Le DKIM

DKIM (DomainKeys Identified Mail) est une norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique. Elle constitue une protection efficace contre le spam et l'hameçonnage.

DKIM fonctionne par signature cryptographique du corps du message ou d'une partie de celui-ci et d'une partie de ses en-têtes. Une signature DKIM vérifie donc l'authenticité du domaine expéditeur et garantit l'intégrité du message. **Source Wikipédia**

La mise en place s'effectue par l'usage d'échange de clé privée/clé publique avec le fournisseur de la passerelle SMTP et l'enregistrement par le client d'une entrée dans sa zone DNS de type :

service._domainkey.domain.tld IN TXT v=DKIM1; p=LaCléFournieParLePrestataire

Passerelles SMTP reconnues

N’importe qui peut déployer son propre serveur SMTP pour effectuer ses envois de mails.

La bonne réception des mails passe aussi par la réputation des IPs des serveurs SMTP.

Un opérateur connu, aura envoyé un volume suffisamment significatif de mails pour que celui-ci soit reconnu par les plateformes distantes et les anti-spam & RBL et ne soit pas considéré comme émetteur de spam

En cas de mauvaise réputation, les IPs seront enregistrées comme émettrice de spam et bloquées par la plupart des serveurs de messagerie. Il est alors très compliqué, lorsque l’on n’est pas un acteur du marché, de se retirer de ces listes.

Les opérateurs ont également des IPs de secours, permettant, en cas de blacklistage d’une de leurs IPs, de basculer sur une autre IP.

En résumé

Ce qu'il faut faire :

- ✔ Envoyer ses campagnes avec une adresse email existante
- ✔ Bien relire ses mails et vérifier la validité des liens
- ✔ Faire attention à la casse des mots, le ratio texte/image
- ✔ S'assurer d'avoir fait les déclarations SPF et DKIM pour les serveurs utilisés

Merci pour votre écoute,
Olivier GILLES

ogilles@alinto.eu

https://linkedin.com/in/olivier-gilles-307493127

Questions / Réponses